NIH Web Page Privacy Policy

A. PURPOSE

This chapter establishes policies and procedures for ensuring the privacy and protection of personal information on NIH Web sites. This policy also applies to NIH Web sites that are developed and/or maintained by contract personnel. Additional guidance and requirements for the hosting of data on NIH Web servers and acceptable uses for Web pages created for NIH are posted at: http://irm.cit.nih.gov/policy/guideli2.html

B. RESPONSIBILITIES

NIH Institutes and Centers (ICs) must comply with the privacy policies in this chapter prior to posting new or revised Web pages. For example, if an IC Web site states that the information collected will not be available to any other entity, it is the responsibility of the IC to assure that no such sharing takes place. To ensure adherence to this policy, each IC shall review all new Web pages to be posted or altered for compliance with its stated Web privacy policies.

1. IC Program/Content Managers:

   - Provide necessary oversight to IC Web Site Operation Staff and ensure that program Web sites (including those maintained by contract staff) are in compliance with federal law and internal NIH Web policies including policy information contained (or referenced) in this chapter.

2. IC Web Site Operation Staff:

   - Ensure that Web sites that are collecting and maintaining data are doing so in compliance with their web Privacy Notification Statement and in accordance with the requirements contained in this chapter;

   - Ensure that users can easily find and access their web Privacy Notification Statement and that disclaimers are used and visible on their site, when the site contains external links to sites outside NIH.

3. NIH Privacy Act Officer:

   - Advises the NIH Director and IC management on the Privacy Act requirements.

4. IC Privacy Act Coordinators:

   - Assist IC staff in determining when a Privacy Act notification is needed, determining if an existing notification statement can be used, and developing a Web page privacy statement;

- Provide ongoing guidance, as required, on changes to Privacy Act requirements.

5. Oversight of this policy will be carried out through a coordinated effort between the Office of Management Assessment (OMA), Center for Information Technology (CIT), and Office of Communications and Public Liaison (OCPL).

C. DEFINITIONS

1. Child and Children: Unless the context otherwise provides, it means individuals under the age of 18.

2. Contract: Includes any contract, written or oral, subject to the Federal Acquisition Regulations.

3. Cookies: A text file, saved in a browser's directory or folder, which is stored in the computer's memory while the browser is running. The cookie usually goes unnoticed to the user and expire at some point. Using the cookie, the site can collect user preferences. The server generates a cookie, and then the cookie is sent to the user's computer. The browser records the cookie onto a "cookie list." The cookie was developed as a timesaving device to prevent the user from having to manually dispense personal information upon each site visit. It was also developed to allow users to customize their Web service, or to allow Web site creators to gauge the effectiveness of their sites.

Basically there are two types of cookies used on Web pages:

- **"Persistent cookies"**: Collect and maintain information for later use. They can track the activities of users over time and across different Web sites. These are capable of capturing personal information that can be retrieved by individual identifiers (e.g., name, SSN, etc.) and may therefore be covered by the Privacy Act. Use of persistent cookies requires pre-approval in accordance with Section 5 below.

- **"Session cookies"**: Collect information and use it for a single session. These generally would not save information for later retrieval and would not be covered by the Privacy Act.

NIH Web Page Privacy Policy

4. Disclaimer: A Web site statement that states that NIH is not responsible for the information or material included on (1) the NIH Web site that was derived from other non-NIH sources and (2) external Web pages. A disclaimer is also used to avoid giving a user the impression that NIH is endorsing information, or a commercial product described on an NIH page or at an external site linked to an NIH page. Disclaimers on copyright, endorsement (general and external links), liability, and medical information may be used, as appropriate, for individual IC Web sites. See Appendix for sample disclaimers. In determining appropriate statements, careful consideration should be given to the nature of the specific site and its potential liability.

5. Exit Page: An intermediary page the user sees before proceeding to external Web pages not located on NIH servers, and which notifies the user that they are leaving NIH-managed Web pages.

6. FAR: Federal Acquisition Regulation, 48 C.F.R.

7. IC: NIH Institutes and Centers and other components.

8. Kid's Pages: NIH Web sites directed to children under the age of 13.

9. Personal Identifier: A name, or the identifying number, symbol, or other unique identifier, such as Social Security Number or User ID Number assigned to an individual.

10. Personally Identifiable Information: Information retrieved by a personal identifier.

11. Privacy Act: Privacy Act of 1974, as amended (5 U.S.C. 552a).

12. Privacy Act System of Records: A set or subset of records under the control of NIH or the IC, containing personal information (including, but not limited to, education, financial transactions, medical history, and criminal or employment history), from which a personal identifier retrieves information.

13. Secretary: The Secretary of Health and Human Services (HHS).

14. Verifiable Parental Consent: Consent from the child's parent or legal guardian, verified by reasonable efforts of Kids' Pages IC Program/Content Manager in coordination with the IC Web Site Operation Staff (taking into consideration available technology), shall be obtained before collecting, using, or disclosing personal information from or about a child. Verifiable Parental Consent is used to ensure that before personal information is collected from a child, a parent or guardian of the child receives notice of the operator's information practices and consents to those practices.

NIH Web Page Privacy Policy

D. POLICY

1. General Requirements

a. NIH ICs and other components must post clear privacy policies on top-level/principal Web sites, including NIH and IC-level sites, major on-line public resource sites and any other known major public entry points, as well as any Web page that collects or posts personal information.

b. Web sites that collect or sponsor a collection of information on identical items from 10 or more respondents must comply with the requirements of NIH Manual Chapter 1825, "Information Collection from the Public" located at: http://www1.od.nih.gov/oma/manualchapters/management/1825

c. Privacy policy links must be clearly labeled and easy to access by all visitors to a Web site. If the privacy statement is combined with other mandated or recommended Web site statements or information, the link should be labeled accordingly, e.g., Privacy/Disclaimers.

d. In general, privacy policies must clearly and concisely inform visitors to the site about:

(1) Any personal information collected about the individual or proposed to be collected;
(2) Why the information is collected;
(3) How the information is collected (if not apparent);
(4) How the visitor can avoid or disable the collection mechanism if so desired;
(5) How the information that is collected will be used, including retention and disposition information;
(6) Who the visitor can contact to access the information collected about them.

For Web sites that are set up to collect personally identifiable information and retrieve it by personal identifier (records covered by the Privacy Act) or for access/interaction by children, additional requirements must be followed and are discussed in Section D.3.

2. Privacy Act Requirements

An NIH Web site that uses mechanisms that collect and maintain personally identifiable information from individuals who visit the Web site, e.g., surveys, cookies (see Section C.3. above), Web server logs, and other mechanisms, must first have a valid Privacy Act System Notice published in the Federal Register which covers the identifiable records.

NIH Web Page Privacy Policy

(Note: Currently, cookies and Web server logs are not covered by the Privacy Act unless the information collected is retrieved by personal identifier).

a. **Develop a Privacy Notification Statement:** Any Web page that collects and/or maintains personally identifiable information that will, in practice, be retrieved by personal identifier, must contain the following information in the privacy statement, and this statement must be on or directly linked to the information collection page:

(1) Authority (whether granted by statute or by executive order of the President) which authorizes the solicitation and/or collection of the information and whether disclosure of this information is mandatory or voluntary;
(2) Purpose of the information collection;
(3) Routine uses for information disclosure (likely or known disclosures of the data; these must be reflected in the published Privacy Act System Notice); and
(4) What effect, if any, there is on the individual for not providing all or part of the requested information.

b. IC Privacy Act Coordinators should be contacted for additional information on Privacy Act requirements, for assistance in using an existing Privacy Act notice, if applicable, or to obtain a new system notice to cover data that is collected on Web sites at: http://oma.od.nih.gov/about/contact/browse.asp

3. Children's Online Privacy Protection Act of 1998 (COPPA) Requirements - Agency "KIDs' Pages" Web Sites Intended for use by Children

NIH Web sites that are set up for the intended use by children or that knowingly collect personal information from children under the age of 13. Web privacy statements are required on both internal and external sites. NIH Web sites shall, in addition to the requirements noted above, comply with the following standards set forth in the COPPA, specifically:

a. **Eliminate or Avoid Unnecessary Data Collection Instruments on "Kids' Pages**." Web sites that collect personally identifiable information from children under age 13 should eliminate or reconsider including the information collection if the information is not essential to the IC program.

b. **Include a Privacy Notice on Every "Kids' Page."** Internal or external Web sites that are set up for the intended use by children or that knowingly collect personal information from children under the age of 13 must contain a notice of the information collection practices (i.e., whether or not they keep/store information) and be in compliance with public information collection requirements (see Section D.1.b. above).

A "Kids' Page" privacy notice must include:

(1) A description of the specific types of personal information you collect directly from children (e.g., name, age, home address, e-mail address or hobbies), and if any additional information is collected passively (e.g., cookies);
(2) A description of how you will use the information, e.g., to make the information available through a child's participation in a chat room, whether personal information is forwarded to third parties;
(3) How long your IC will maintain the information;
(4) Who will have access to the information; and
(5) A contact name and information (address, telephone, e-mail address) for the site.

c. **Get Parental Consent**. ICs must make reasonable efforts (taking into consideration available technology) to ensure that a parent (or legal guardian) of the child receives notice of these information practices and consents to those practices before personal information is collected from a child. (Note: Disclosure of personal information is permitted only to the extent that it has also been included as a "purpose" or "routine use" in an active Privacy Act system of records). Specifically,

(1) The IC must get parental consent when it collects an e-mail address or other personal information and:

(a) Plans to change the kinds of information previously collected;
(b) Changes how the information is used;
(c) Offers the information to new or different third parties;
(d) Uses the information in a way that is different than how it was specified when parental consent was originally obtained; or
(e) Gives a child access to a secondary site that was not originally specified in the Web site notification.

(2) Parental consent is not necessary if the "Kid's Page" site collects an e-mail address to:

(a) Respond to a onetime request from the child and then the e-mail address from the child is deleted, e.g., research poster, responding to an inquiry, and similar requests. Repeated contact with the same child requires consent (see Section D.3.C.1 above);
(b) Contact the parent;
(c) Ensure the safety of the child or the site;
(d) Fulfill a NIH newsletter subscription request for one issue. Continuation of the subscription requires consent.

d. **Provide Instructions to Parents on how to Review, Change, or Delete the Personal Information Collected from their Children, or Revoke their Consent for Further Data Collection.**

(1) Parents have the right to revoke their consent and ask that information about their children be deleted from the site's database at any time. When a parent revokes consent, the Web site must stop collecting, using or disclosing information from that child immediately.

(2) It is also advisable that an exit page be placed between the IC "Kids Page" and any external links. This provides clear notification to the child and parent that they are exiting NIH and that NIH can no longer guarantee the security of their information.

4. Unsolicited (incoming) E-mail Requirements

ICs shall notify users how the site handles unsolicited e-mail, including a notice that the sender should not expect privacy.

The following is a sample statement:

"E-mail sent to NIH may be seen by a number of people who are responsible for answering questions. If you send us an e-mail, you are advised that e-mail is not necessarily secure against interception. So, if your communication includes sensitive information like your Social Security Number or personal health information, you may prefer to contact us by postal mail or telephone rather than e-mail."

5. "Cookie" Technology Requirements

a. Cookies track computer use. "Persistent cookies" track the activities of users over time and across different Web sites. Federal policy states that Federal agencies and their contractors may not use persistent cookies at Federal Web sites unless all of the following conditions are met:

(1) There is a compelling need to gather the data on the site, e.g., site enhancement, navigational assistance for returning visitors, or similar needs;
(2) The IC has received prior approval by the Secretary, for the use of persistent cookies;
(3) The IC provides clear and conspicuous notice about its use of cookies or other automatic means of collecting information; and
(4) The IC includes its Web site appropriate and publicly disclosed privacy safeguards for how information derived from "cookies" will be handled and maintained.

b. To obtain the approval for the use of persistent cookies, an IC must submit a written request to the NIH Privacy Act Officer at the following address:

NIH/OD/OM/OA/Office of Management Assessment
6011 Executive Boulevard, Suite 601
MSC 7669
Rockville, Maryland 20852

The Privacy Act Officer will review the request and forward the request along with a recommendation to the NIH Chief Information Officer (or his/her designee) for NIH clearance. If the persistent cookies will collect and maintain personally identifiable information, see Section D.2. above, for additional Privacy Act requirements.

The following must be included in the request:

(1) A complete description of all information the cookie will collect;
(2) A detailed description of the purpose for the cookie;
(3) How long the cookie will stay on the user's computer;
(4) How the IC will maintain the information collected;
(5) The proposed notice that the IC will display on the cookie Web site (upon approval) that clearly states to the user of the site, information reported in Section D.5.a. 1 - 4 above; and
(6) The name of the contact person for cookie information

(Note: If a contractor develops the Web site, a copy of the approval should be kept in the contract file).

6. Links to non-NIH External Sites

It is recommended that NIH IC Web pages containing links to external Web pages not located on NIH servers provide a disclaimer that states that NIH is not responsible for the material found on, or data collection activities of, these external Web pages. The disclaimer can be conveyed by use of Exit statements; however, other approaches are equally acceptable. Sample Disclaimers are provided at: http://irm.cit.nih.gov/policy/disclsamp.html

7. Contractor Developed, Maintained, or Managed Web Sites

"Contract" covers any contract subject to the Federal Acquisition Regulations (FAR). When an agency contracts for the design, development, or operation of a Web page necessary to accomplish an NIH function, the IC must apply the requirements of this policy to the contract. Web pages operated under a contract, which are designed to

accomplish an NIH function, are, in effect, deemed to be maintained by the agency.

Contracts that require the contractor to maintain a system of records covered by the Privacy Act, i.e., when the records will contain personal information that is retrieved by an individual identifier, the system of records must state that the Privacy Act applies and include appropriate FAR citations, e.g., FAR 52.224.

Contracts for the development, maintenance, or management of NIH Web sites shall include certain language (see Appendix for sample language).

E. REFERENCES

1. Privacy Act of 1974, as amended, 5 U.S.C. 552a at: http://www.usdoj.gov/foia/privstat.htm
2. Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503)
3. Computer Security Act of 1987 (Public Law 100-235)
4. Freedom of Information Act, as amended, 5 U.S.C. 552
5. Information Technology Management Reform Act of 1996 (40 U.S.C. 1401 et seq.) at: http://irm.cit.nih.gov/policy/itmra.html
6. Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501 et seq.), and implementing regulations (16 CFR Part 312) at: http://www.ftc.gov/ogc/coppa1.htm
7. FTC Guidance, “How to Comply With The Children's Online Privacy Protection Rule,” (November, 1999) at: http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm
8. World Wide Web - NIH Guidance at: http://irm.cit.nih.gov/policy/guideli2.html
9. OMB Circular A-130, “Management of Federal Information Resources,” at: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
10. OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000) at: http://www.whitehouse.gov/omb/memoranda/m00-13.html
11. OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999) at: http://www.whitehouse.gov/omb/memoranda/m99-18.html
12. NIH Manual Chapter 1825, “ Information Collection from the Public,” at: http://www1.od.nih.gov/oma/manualchapters/management/1825

F. RECORDS RETENTION AND DISPOSAL

All records (e-mail and non-e-mail) pertaining to this chapter must be retained and disposed of under the authority of NIH Manual 1743,"Keeping and Destroying Records”, Appendix 1, "NIH Records Control Schedule," in accordance with the specific schedule item as applied to the kind of records.

NIH e-mail messages, including attachments that are created on NIH computer systems or transmitted over NIH networks that are evidence of the activities of the agency or have informational value are considered Federal records. These records must be maintained in

accordance with current NIH Records Management guidelines. The IC Records Officer should be contacted for additional information.

All e-mail messages are considered Government property, and, if requested for a legitimate Government purpose, must be provided to the requester. Employees' supervisors, NIH staff conducting official reviews or investigations, and the Office of Inspector General may request access to or copies of e-mail messages. E-mail messages must also be provided to Congressional oversight committees if requested and are subject to Freedom of Information Act requests.

Since most e-mail systems have back-up files that are retained for significant periods of time, e-mail messages and attachments are likely to be retrievable from a back-up file after they have been deleted from an individual's computer. The back-up files are subject to the same requests as the original messages.

G. MANAGEMENT CONTROLS

The purpose of this manual issuance is to provide guidance to ICs in meeting requirements related to privacy and the protection of personal information on NIH Web pages.

Overview of this policy will be carried out through a coordinated effort between the Center for Information Technology (CIT), Office of Management Assessment (OMA), and Office of Communications and Public Liaison (OCPL).

Appropriate management controls must be in place before a Web page may be activated. Developers and contractors developing NIH Web pages are responsible for ensuring compliance within the ICs.

Each year, a workgroup of members from OMA, CIT and OCPL will survey a sample of NIH Web sites for compliance of these policies. External reviews may be used as alternative reviews for this purpose. Review Reports shall be sent to the NIH Deputy Director for Management (DDM).

NIH Web Page Privacy Policy

CONTRACT ARTICLE H – SAMPLE LANGUAGE

Text for use in all acquisitions where the contractor is required to develop, maintain, operate or manage a Web site on behalf of the government.

Under Federal Information Technology policy, Web sites owned or operated by or for the government must post clear privacy policies on top-level/principal Web sites, including NIH and Institute/Center-level sites, major on-line public resource sites and any other known major entry points. Web sites that are owned or operated by a contractor on behalf of the NIH that implement and use mechanisms that collect and maintain personally identifiable information from individuals who visit the Web site, e.g., cookies, Web server logs, surveys, and similar mechanisms, may not use that information to identify specific individuals without a valid Privacy Act System Notice published in the Federal Register, which covers the identifiable records. (Note: Currently, cookies and Web server logs are not covered by the Privacy Act unless the information collected is then used to identify specific individuals).

"Personally identifiable" information includes information that can be linked to a specific individual, e.g., name, Social Security Number, User ID number.

NIH IC Web pages containing links to external Web pages not located on NIH servers should include a link to an Exit statement that disclaims NIH responsibility for the protection of privacy and material included in the external Web pages. Sample Disclaimers are available at: http://irm.cit.nih.gov/policy/disclsamp.html

Web pages that are directed to children under the age of 13 have additional requirements as provided in the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.), and implementing regulations (16 CFR 312) available at: http:///www.ftc.gov/ogc/coppa1.htm

Additional guidance and requirements for the publication of data on NIH Web servers and acceptable uses for Web pages created for NIH is posted at: http://irm.cit.nih.gov/policy/guideli2.html